WHAT IS CLAIMED IS:

1. A system for maintaining security in a distributed computing environment, comprising:

a policy manager for managing a security policy; and

an application guard for managing access to securable components as specified by the security policy.

2. The system of claim 1, wherein said policy manager comprises a management station for constructing and editing the security policy.

3. The system of claim 2, wherein said policy manager further comprises a distributor for distributing the security policy to a client.

4. The system of claim 2, wherein said policy manager further comprises a distributor for distributing a customized local policy based on the security policy to a client.

5. The system of claim 4, wherein said policy manager further comprises a logger for recording and tracking authorization events that occur through the application guard.

6. The system of claim 4, wherein the policy manager further comprises a database management system for maintaining the security policy.

7. The system of claim 4, wherein the customized local policy is optimized.

8. The system of claim 1, wherein said securable components are selected from the group consisting of: at least one application, a function within an application, a procedure within an application, a data structure within an application, a database object referenced by an application, or a file system object referenced by an application.

9. The system of claim 1, wherein said system is scalable by further comprising a plurality of clients, said policy manager further managing and distributing a customized local policy to each client, and at least one additional application guard located on each client for managing access to the securable components as specified by each customized local policy.

10. The system of claim 1, wherein said application guard includes an application guard interface coupled to an application for requesting access to the securable components, and at least one authorization engine for evaluating requests from the application guard interface as specified by a customized local policy based on the security policy.

11. The system of claim 10, wherein said application guard interface is located on a client, and said at least one authorization engine and said customized local policy are located on a client server.

12. The system of claim 1, wherein the security policy is defined by a policy language to grant or deny access to the securable components for a particular user.

13. The system of claim 1 further comprising a policy loader for bulk loading the security policy onto the system.

14. The system of claim 1, wherein said policy manager includes a set of menu options to manage and distribute the security policy.

15. The system of claim 14, wherein said set of menu options include: navigate tree, analyze policy, edit policy, distribute policy, and view audit log.

16. The system of claim 1, wherein the application guard further allows for additional customized code to process and evaluate authorization requests based on the additional customized code.

17. The system of claim 1, wherein the policy manager further includes a policy manager application guard for managing access to the policy manager as specified by a local administrative policy.

18. A system for controlling user access in a distributed computing environment, comprising:

a global policy specifying access privileges of the user to securable components;

a policy manager located on a server for managing and distributing a local client policy based on the global policy to a client, and

an application guard located on the client for managing access to the securable components as specified by the local client policy.

19. The system of claim 18 further comprising at least one additional client, said policy manager further managing and distributing a customized local policy based on the global policy to each additional client, and at least one additional application guard located on each additional client for managing access to the securable components as specified by the customized local policy.

20. The system of claim 18, wherein said policy manager comprises:

a management station for constructing and editing the global policy; and

a distributor for distributing the local policy to the client.

21. The system of claim 20, wherein said policy manager further comprises a database management system for maintaining the global policy.

22. The system of claim 18, wherein said policy manager further comprises a logger for recording and tracking authorization events that occur through the application guard.

23. The system of claim 18, wherein said securable components are selected from the group consisting of: at least one application, a function within an application, a procedure within an application, a data structure within an application, a database object referenced by an application, or a file system object referenced by an application.

24. The system of claim 18, wherein the global policy is defined by a policy language to grant or deny access to the securable components for a particular user.

25. The system of claim 18, wherein said system is scalable by further comprising a plurality of clients, said policy manager further managing and distributing a customized local policy to each client, and at least one additional application guard located on each client for managing access to the securable components as specified by each customized local policy.

26. The system of claim 18, wherein said application guard includes an application guard interface coupled to an application for requesting access to the securable components, and at least one authorization engine for evaluating requests from the application guard interface as specified by the local client policy.

27. The system of claim 18 further comprising a policy bulk loader for bulk loading the global policy onto the system.

28. The system of claim 18, wherein the local client policy is optimized.

29. The system of claim 18, wherein the application guard further allows for additional customized code to process and evaluate authorization requests based on the additional customized code.

30. The system of claim 18, wherein the policy manager further includes a policy manager application guard for managing access to the policy manager as specified by a local administrative policy.

31. A system for authorization that provides access to securable components for a user, comprising:

a policy specifying access privileges of the user to the securable components;

an application guard; and

a processor coupled to said system, said processor executing said application guard to manage access to the securable components.

32. The system of claim 31 further including an audit log for recording and tracking each authorization event that occurs though the application guard.

33. The system of claim 31, wherein said securable components are selected from the group consisting of: at least one application, a function within an application, a procedure within an application, a data structure within an application, a database object referenced by an application, or a file system object referenced by an application.

34. The system of claim 31, wherein said application guard comprises an application guard interface connected to an application for managing access to the securable components in said application.

35. The system of claim 31, wherein the application guard further allows for additional customized code to process and evaluate authorization requests based on the additional customized code.

36. The system of claim 31, wherein said application guard includes an application guard interface coupled to an application for requesting access to the securable components, and at least one authorization engine for evaluating requests from the application guard interface as specified by a customized local policy based on the policy.

37. The system of claim 36, wherein said application guard interface is located on a client, and said at least one authorization engine and said customized local policy are located on a client server.

38. A system for managing security in a distributed computing environment, comprising:

a policy manager; and

a processor coupled to said system, said processor executing said policy manager to manage and distribute a customized local policy based on a global policy to a client.

39. The system of claim 38, wherein said policy manager comprises a management station for constructing and editing the global policy.

40. The system of claim 39, wherein said policy manager further comprises a distributor for distributing the customized local policy to the client.

41. The system of claim 38, wherein said policy manager further comprises a logger for recording and tracking authorization events that are received from the client.

42. The system of claim 38, wherein said global policy specifies access privileges of at least one user to securable components.

43. The system of claim 38, wherein the policy manager comprises a database management system for maintaining the global policy.

44. The system of claim 38, wherein the global policy is defined by a policy language to grant or deny access to securable components for a particular user.

45. The system of claim 38, wherein said policy manager includes a set of menu options to manage and distribute the customized local policy.

46. The system of claim 38, wherein the customized local policy is optimized.

47. The system of claim 38, wherein the policy manager further includes a policy manager application guard for managing access to the policy manager as specified by a local administrative policy.

48. A method for maintaining security in a distributed computing environment, comprising the steps of:

managing a policy using a policy manager by specifying access privileges of a user to securable components; and

distributing the policy to a client having an application guard, whereby the application guard manages access to the securable components as specified by the policy.

49. The method of claim 48, further including the step of recording authorization events that occur through the application guard after distributing the policy.

50. The method of claim 48, wherein the securable components are selected from the group consisting of: at least one application, a function within an application, a procedure within an application, a data structure within an application, a database object referenced by an application, or a file system object referenced by an application.

51. A method for maintaining security on a client in a distributed computing environment, comprising the steps of:

constructing and issuing an authorization request for a user to access to securable components located on the client using an application guard;

evaluating the authorization request using the application guard to determine if the authorization request is valid or invalid; and

allowing access to the user via the application guard if the evaluated authorization request was valid, and denying access to the user via the application guard if the authorization request was invalid.

52. The method of claim 51, after evaluating the authorization request, further including the step of recording the authorization request in an audit log.

53. A computer-readable medium comprising program instructions for maintaining security in a distributed computing environment by performing the steps of:

managing a policy using a policy manager by specifying access privileges of a user to securable components;

distributing the policy using the policy manager to a client having an application guard, whereby the application guard manages access to the securable components as specified by the policy; and

executing said policy manager with a processor to manage and distribute the policy.

54. A computer-readable medium comprising program instructions for maintaining security on a client in a distributed computing environment by performing the steps of:

constructing and issuing an authorization request for a user to access to securable components located on the client using an application guard;

evaluating the authorization request using the application guard to determine if the authorization request is valid or invalid;

allowing access to the user via the application guard if the evaluated authorization request was valid, and denying access to the user via the application guard if the authorization request was invalid; and

executing said application guard with a processor to automatically maintain security on the client.

55. A system for maintaining security in a distributed computing environment, comprising:

means for managing a policy using a policy manager by specifying access privileges of a user to securable components;

means for distributing the policy using the policy manager to a client having an application guard, whereby the application guard manages access to the securable components as specified by the policy; and

means for executing the policy manager to manage and distribute the policy.

56. A system for maintaining security on a client in a distributed computing environment, comprising:

means for constructing and issuing an authorization request for a user to access to securable components located on the client using an application guard;

means for evaluating the authorization request using the application guard to determine if the authorization request is valid or invalid;

means for allowing access to the user via the application guard if the evaluated authorization request was valid, and denying access to the user via the application guard if the authorization request was invalid; and

means for executing said application guard to automatically maintain security on the client.